

Vervolgonderzoek: Misbruik van (persoons)gegevens

Een audit naar omgang met BRP-gegevens | Overzicht van Bevindingen

Afdeling Interne Audit en Beleidsonderzoek | December 2025

Samenvatting

Achtergrondinformatie

Om de inwoners van Amsterdam goed van dienst te kunnen zijn, maakt de gemeente gebruik van informatie uit een landelijk stelsel van tien basisregistraties. Deze basisregistraties bevatten essentiële gegevens die nodig zijn voor het uitvoeren van wettelijke taken. Eén van deze registraties is de Basisregistratie Personen (BRP), waarin gegevens zoals naam, geboortedatum, geslacht, nationaliteit en verblijfsplaats zijn opgenomen.

De gemeente Amsterdam is wettelijk verplicht om deze gegevens te gebruiken bij het uitvoeren van haar taken. Deze informatie is cruciaal om een vreedzaam en goed functionerend samenleven in de stad mogelijk te maken. Het is echter van groot belang dat zorgvuldig en integer met deze gegevens wordt omgegaan. Misbruik, ongeoorloofde verkoop of onrechtmatig raadplegen van deze informatie schaadt het vertrouwen van burgers in de overheid.

Aanleiding

Het Gemeentelijk Managementteam (GMT) heeft opdracht gegeven om een vervolgonderzoek uit te voeren naar de risico's van misbruik van vertrouwelijke gegevens binnen de gemeentelijke organisatie. Deze opdracht is gebaseerd op twee belangrijke aanleidingen. Ten eerste betreft het de uitvoering van aanbevelingen uit het beleidsonderzoek naar corruptie uit 2024. Ten tweede zijn er twee incidenten geweest waarbij gegevens uit de Basisregistratie Personen (BRP) zijn gelekt naar het criminele circuit. Deze incidenten vonden plaats in het najaar van 2024 en het voorjaar van 2025.

De afdeling Interne Audit en Beleidsonderzoek (IA&BO) is verantwoordelijk voor het uitvoeren van dit onderzoek, dat plaatsvindt in de vorm van een audit met twee fasen. In de eerste fase is een QuickScan uitgevoerd om gedrags- en cultuurfactoren (soft controls) binnen de organisatie in kaart te brengen. In de tweede fase is verder onderzoek gedaan naar hard controls en is een verdieping aangebracht in de analyse van soft controls. Voor deze audit zijn ongeveer zestig gesprekken gevoerd en is relevante documentatie bestudeerd.

Toelichting hard controls en soft controls (zie voor meer uitleg bijlage 1)

De beheersing van risico's op misbruik van persoonsgegevens steunt op een combinatie van hard controls en soft controls. Hard controls zijn formele, tastbare maatregelen die zijn ontworpen om de verstrekking, toegang, het gebruik en het toezicht op BRP-gegevens te waarborgen. Soft controls richten zich op de organisatiecultuur welke wordt gereflecteerd in gedrag van medewerkers en leidinggevenden. Soft controls versterken hard controls door gewenst gedrag te stimuleren, ongewenst gedrag tegen te gaan en een bijdrage te leveren in het tijdig signaleren van risico's. Een goede balans tussen hard en soft controls is essentieel om zowel technische als gedragsmatige risico's effectief te beheersen en een veilige omgang met persoonsgegevens te waarborgen.

Doelstelling

De doelstelling van deze audit is inzicht bieden in de beheersing van het risico op misbruik van persoonsgegevens vanuit de BRP door na te gaan of de aanwezige beheersmaatregelen het risico in voldoende mate afdekken.

Hoofdvraag en deelvragen

Hoofdvraag:

Wordt het risico op misbruik van persoonsgegevens vanuit de BRP in voldoende mate beheerst en welke lessen kunnen worden getrokken om de bescherming van persoonsgegevens verder te verbeteren?

Deelvragen:

1. Hard controls: Hoe zijn de toegangsrechten, het gegevensgebruik en de monitoring binnen de BRP technisch en organisatorisch ingericht en in hoeverre sluiten deze aan bij het principe van 'least privilege' en het effectief detecteren van ongeautoriseerd gedrag?
2. Soft controls: Hoe is de beheersing van gedrags- en cultuur gerelateerde factoren vormgegeven bij het omgaan met persoonsgegevens uit de BRP?
3. Verbeteringen: Welke lessen kunnen we trekken voor het verder verbeteren van de beheersing rondom het gebruik van de BRP op de aspecten gedrag, gegevenstoegang, gegevensgebruik en monitoring?

Scope (zie voor meer detail bijlage 2)

Deze audit richt zich op de beheersmaatregelen die borgen dat persoonsgegevens in iBurgerzaken of via de Makelaarssuite (MKS) uitsluitend door bevoegde medewerkers en voor gemeentelijke processen worden geraadpleegd bij de directies Belastingen, Dienstverlening, Werk en Participatie, Inkomen en Toezicht Handhaving Openbare Ruimte (THOR).

Conclusie

Het risico op misbruik van persoonsgegevens vanuit de BRP wordt op dit moment onvoldoende beheerst. Tegelijkertijd laat het onderzoek zien dat een aantal randvoorwaarden voor zorgvuldige omgang met BRP-gegevens deels aanwezig is. Zo zijn de afspraken over gegevensverstrekking vastgelegd in convenanten en transparantiedocumenten, die vooraf worden gereviewd door privacy officers, informatiebeveiligingsadviseurs en betrokken directies. Daarnaast is bij incidenten sprake van opvolging.

Zowel de hard controls als de soft controls vertonen echter duidelijke tekortkomingen. Met name het gebrek aan technische beperkingen in toegang tot gegevens en het ontbreken van begrenzing van de zoekmogelijkheden in de BRP-gegevens, onvoldoende toegangsbeheer, beperkte aanvullende maatregelen voor toegang en het ontbreken van actieve monitoring zorgen ervoor dat er onvoldoende structurele waarborgen zijn om onrechtmatig gebruik te voorkomen of tijdig te signaleren. Door het ontbreken van effectieve hard controls worden leidinggevenden niet adequaat gefaciliteerd in het toezicht op en de sturing van gewenst gedrag in de omgang met BRP-gegevens, waardoor ruimte ontstaat voor nieuwsgierig of kwaadwillend gedrag van medewerkers.

Daarbij is het van belang te onderkennen dat de beheersing van BRP-gegevens binnen de directies complex is. De gemeente is ook afhankelijk van landelijke ontwikkelingen en van doorontwikkeling bij softwareleveranciers waardoor mogelijkheden om toegang, zoekgedrag en monitoring technisch te beperken, moeilijker is in te regelen.. Deze technische beperkingen maken dat een belangrijk deel van de beheersing in de praktijk leunt op organisatorische en gedragsmatige maatregelen binnen de directies.

Tegelijkertijd versterken gebreken in soft controls, met name onvoldoende training en bewustwording, gebrek aan duidelijkheid en voorbeeldgedrag, beperkte bespreekbaarheid en aanspreekcultuur en het ontbreken van structureel toezicht en handhaving, het risico op misbruik van persoonsgegevens doordat medewerkers onvoldoende worden ondersteund en beschermd.

Een betere integratie van zowel hard controls als soft controls is noodzakelijk om het risico op misbruik effectief te beheersen. Uit de gesprekken is bovendien naar voren gekomen dat medewerkers onrechtmatige raadplegingen uitvoeren, wat de noodzaak onderstreept van een integrale aanpak waarbij zowel hard controls als soft controls worden versterkt en beter op elkaar worden afgestemd.

Samenvatting bevindingen

De hard controls bieden onvoldoende structurele waarborgen voor een adequate beheersing van het risico op misbruik van BRP-gegevens. Zo ontbreken technische beperkingen in het systeem, is het toegangsbeheer onvoldoende, zijn er slechts beperkte aanvullende maatregelen voor toegangsverlening en ontbreekt het aan volledige logging en actieve monitoring.

- Het ontbreken van technische beperkingen in het systeem heeft twee gevolgen. Ten eerste hebben medewerkers toegang tot persoonsgegevens van alle inwoners van Nederland. Dit betekent dat medewerkers toegang hebben tot meer informatie dan zij nodig hebben voor de uitoefening van hun functie. Ten tweede kunnen zij vrij zoeken in BRP-gegevens zonder koppeling aan een toegewezen werkvoorraad of dossier. Dit tezamen vergroot de kans op misbruik van BRP-gegevens en bemoeilijkt het toezicht op het correct omgaan met de verstrekte informatie.
- Daarnaast is het toegangsbeheer onvoldoende. Autorisatiematrixen zijn niet consistent vastgesteld of actueel, wat leidt tot onduidelijkheid over wie toegang heeft tot welke gegevens. Ook worden toegangsrechten niet tijdig ingetrokken bij uitdiensttreding of langdurige afwezigheid, waardoor de kans op onrechtmatig raadplegen van persoonsgegevens wordt vergroot. Bovendien worden stedelijke processen voor logisch toegangsbeheer niet nageleefd, wat de controle op en het beheer van toegangsrechten verder bemoeilijkt.
- Verder zorgen beperkte aanvullende maatregelen voor toegang ervoor dat medewerkers toegang krijgen tot BRP-gegevens zonder dat zij goed op de hoogte worden gesteld van de regels en voorwaarden in omgang met deze gegevens. Dit betekent dat medewerkers mogelijk onvoldoende kennis en bewustwording hebben over de juiste omgang met persoonsgegevens, wat het risico op onzorgvuldig of onrechtmatig gebruik vergroot.
- Het ontbreken van volledige logging, zoals het ontbreken van dossiercodes, zorgt ervoor dat het niet mogelijk is om raadplegingen direct te koppelen aan een werkvoorraad of een dossier wat het signaleren van afwijkend gedrag als onderdeel van actieve monitoring bemoeilijkt. Zonder deze informatie is het voor leidinggevenden en vrijwel onmogelijk om effectief toezicht te houden op het gebruik van BRP-gegevens.

Daarnaast zijn ook tekortkomingen in soft controls vastgesteld. Onvoldoende training en bewustwording, gebrek aan duidelijkheid en voorbeeldgedrag, beperkte bespreekbaarheid en aanspreekcultuur en het gebrek aan toezicht en bekrachtiging zorgen ervoor dat medewerkers onvoldoende worden ondersteund, beschermd, en indien nodig, gecorrigeerd.

- Sommige medewerkers, vooral voormalige uitzendkrachten, volgen de verplichte e-learning gedragscode over omgang met informatie pas na het in directe dienst treden bij gemeente Amsterdam. Daarnaast is de training bij aanvang van het werk vooral gericht op inhoudelijke taken en nauwelijks op de omgang met BRP-gegevens. Hierdoor missen medewerkers kennis over hoe zij zorgvuldig met persoonsgegevens moeten omgaan. Dit vergroot de kans op fouten en onzorgvuldig gebruik van BRP-gegevens.

- De regels over de omgang met en het delen van BRP-gegevens met collega's bevatten grijze gebieden, waardoor onduidelijkheid ontstaat. De aanwezige richtlijnen over de omgang met BRP-gegevens staan niet op papier en worden
- niet structureel en periodiek gecommuniceerd. Ook is er een discrepantie tussen het (voorbeeld)gedrag dat leidinggevenden zeggen te vertonen en hoe dat door medewerkers wordt ervaren. De goede gedragingen die de leidinggevenden laten zien, worden door medewerkers niet gekoppeld aan de omgang met de BRP. Door het gebrek aan duidelijkheid en voorbeeldgedrag weten medewerkers niet goed wat wel en niet mag. Dit ondermijnt het belang van zorgvuldige omgang met persoonsgegevens en vergroot de kans op onjuist gebruik.
- Knelpunten worden niet structureel besproken in teamverband en zowel medewerkers als leidinggevenden spreken elkaar beperkt aan op omgang met BRP-gegevens. Dit terwijl in de interviews naar voren is gekomen dat medewerkers vanuit nieuwsgierigheid of voor privégebruik soms BRP-gegevens raadplegen voor niet direct werk gerelateerde redenen. Het gebrek aan bespreekbaarheid en aanspreekbaarheid belemmert het leren van fouten en het corrigeren van ongewenst gedrag.
- Door een gebrek aan informatie hebben leidinggevenden en collega's beperkt zicht op het raadpleeggedrag van medewerkers in BRP-gegevens. Daarnaast ontbreekt structureel toezicht op het gebruik van deze gegevens, waardoor leidinggevenden niet in staat zijn om medewerkers aan te spreken. Tot slot vindt bekrachtiging plaats bij ernstige gevallen en is positieve bekrachtiging ten aanzien van BRP-gebruik beperkt. Zonder structureel toezicht is het niet mogelijk om afwijkend gedrag tijdig te signaleren. Dit vergroot de kans dat onrechtmatig gebruik van persoonsgegevens onopgemerkt blijft.

In de huidige situatie versterken de tekortkomingen in hard controls en soft controls elkaar. Door technische beperkingen en beperkte monitoring wordt afwijkend gedrag niet of te laat wordt gesignaleerd. Tegelijkertijd zorgt het gebrek aan training, duidelijkheid van de regels en aanspreekcultuur ervoor dat medewerkers niet of onvoldoende worden ondersteund, beschermd, en indien nodig, gecorrigeerd om zorgvuldig met persoonsgegevens om te gaan. Met als gevolg dat het risico op misbruik van persoonsgegevens vanuit de BRP op dit moment onvoldoende wordt beheerst. Ondanks de technische beperkingen die deels ook buiten de invloedsfeer van de gemeente zelf liggen, zien wij verschillende aanknopingspunten om de beheersing te versterken. Ook door relatief kleine veranderingen in gedrag van zowel medewerkers als leidinggevenden en de daarvoor noodzakelijke randvoorwaarden kan een meer integere omgang met gegevens uit de BRP worden bereikt.

1. Hard Controls

Introductie hard controls



In deze audit worden de formele tastbare maatregelen aangeduid als hard controls. Er is onderzoek gedaan naar gegevensverstrekking, toegangsverlening, gegevensgebruik en toezicht met behulp van monitoring en logging.

1.1. Gegevensverstrekking

Achtergrond

De gemeente heeft de verantwoordelijkheid voor de distributie van BRP-gegevens belegd bij directie Data, die tevens stelselverantwoordelijke is voor de basisregistraties. De gemeente Amsterdam is verplicht om voor al haar wettelijke taken gebruik te maken van de gegevens die zijn vastgelegd in basisregistraties, zoals de Basisregistratie Personen (BRP). Om dit mogelijk te maken, is directie Data verantwoordelijk voor het verspreiden van gegevens uit de basisregistraties naar de directies die ze nodig hebben voor hun taken. De directie Data bepaalt ook welke gegevens beschikbaar worden gesteld en zorgt ervoor dat dit altijd gebeurt in overeenstemming met de wet- en regelgeving. Directie Data beslist welke gegevensvelden (bijvoorbeeld geboortedatum of adres) en welk deel van de database (de personenset, een objectief afgebakende deelverzameling van de personen geregistreerd in de database) beschikbaar wordt gesteld.

De persoonsgegevens van inwoners van Amsterdam worden beheerd door de directie Dienstverlening in de lokale BRP. Voor gegevens van inwoners buiten Amsterdam maakt de gemeente gebruik van de landelijke BRP, aangeduid als BRP-V en beheerd door de Rijksdienst voor Identiteitsgegevens (RvIG).

Gegevens kunnen via drie routes beschikbaar worden gesteld: (1) toegang tot het BRP-raadpleegscherm in Makelaarssuite, binnenkort vervangen door BenK-BRP, (2) toegang tot BRP-gegevens via een applicatiekoppeling benaderbaar vanuit de taakapplicatie van een directie en (3) het verstrekken van bestanden. Deze audit beperkt zich tot 2 van deze 3 distributiekanalen, namelijk gegevensverstrekking via het Raadpleegscherm en via de applicatiekoppeling. Het verstrekken van bestanden is buiten scope gehouden omdat bij bestandsverstrekking geen sprake is van grote groepen medewerkers die 24/7 toegang tot individuele persoonsgegevens hebben.

Bevinding 1: Adequaat ingericht proces voor gegevensverstrekking

Directie Data ontvangt van een directie een verzoek tot het beschikbaar stellen van BRP-gegevens. Vervolgens wordt een proces gestart waarin wordt besproken voor welke

gemeentelijke taak de gegevens nodig zijn, op basis van welke wet- en regelgeving de BRP-gegevens mogen worden verstrekt, welke specifieke soorten informatie (gegevensvelden zoals naam, adres of geboortedatum) en welk deel van de database (personenset, bijvoorbeeld een specifiek stadsdeel) beschikbaar wordt gesteld, aan wie de gegevens worden verstrekt en via welk distributiekanaal dit gebeurt. De afspraken worden vastgelegd in een transparantiedocument, dat een bijlage vormt bij het convenant voor gegevenslevering. De conceptafspraken worden gereviewed door privacy officers, informatiebeveiligingsadviseurs (ISO's) en door deskundigen van directie Data en de afnemende directie.

Bij gebruik van een applicatiekoppeling wordt een positieve assurancerapportage van een aansluitaudit verlangt. Onderdeel van de aansluitaudit is de review van de rapportage van de pen- en hacktest.

De formalisatie van de gegevenslevering bestaat uit een besluit tot gegevenslevering ondertekend door de directeur Data, en de ondertekening van het leveringsconvenant door de directeur Data en de directeur van de afnemende directie. Het transparantiedocument vormt een bijlage bij het convenant met besluit, maar wordt niet geparafeerd. Het paraferen en dateren van bijlagen bij een convenant bevordert de helderheid over welke versie de definitieve afspraken bevat.

Transparantiedocumenten en convenanten worden herzien op verzoek van de directie of wanneer omstandigheden zoals grote wijzigingen daartoe aanleiding geven.

Bevinding 2: Zeer beperkte technische beperking in beschikbaarheid personenset

Na verlenen van toegang hebben medewerkers van een directie in beginsel toegang tot de gegevens van alle inwoners van Nederland. Wel is filtering aanwezig op basis van gegevensveld.

Hiermee kan de hoeveelheid verstrekte gegevens per persoon worden beperkt, maar ook de toegang tot personen met een geheim adres (veldnaam bevat 'inclusief geheim') of van overleden personen (veldnaam bevat 'inclusief overleden').

De gemeente maakt gebruik van de applicatie Makelaarssuite voor de distributie van gegevens vanuit meerdere basisregistraties, zoals de BRP en de RNI (Registratie Niet-Ingezetenen). De applicatie Makelaarssuite wordt vanaf Q4-2025 in stappen vervangen door de applicatie BenK-BRP.

Op basis van het concept-transparantiedocument wordt een inrichting samengesteld voor testdoeleinden. Na afronding van de formele besluitvorming geeft directie Data de opdracht om de inrichting live te zetten in de productieomgeving.

Voor de onderzochte directies zijn afnemersconvenanten met transparantiedocument aangetroffen. In de transparantiedocumenten staat expliciet vermeld voor welke groep van personen gegevens opgezocht mogen worden. Er is echter geen technische beperking, zoals filtering of whitelisting[1], op de beschikbaar gestelde personenset aangetroffen in de inrichting van zowel het BRP-raadpleegscherm als de verstrekking via de koppelingen. Dit betekent dat bij livegang van het BRP-raadpleegscherm of de applicatiekoppeling de medewerkers (met autorisatie) van iedere afnemende directie toegang krijgen tot de persoonsgegevens van alle personen geregistreerd in de BRP.

Risico

Als gevolg van het ontbreken van een technische beperking in de beschikbaar gestelde personenset bestaat de mogelijkheid dat medewerkers gegevens van meer personen opzoeken dan noodzakelijk voor de uitvoering van de toegewezen werkzaamheden. Dit kan leiden tot ongerechtvaardigde gegevensverwerking en uiteindelijk beschadiging van het vertrouwen van burgers en datalekken.

Mogelijke oorzaken

Het aanbrengen van een technische beperking in de beschikbaar gestelde personenset tot personen welke opgenomen zijn in de werkvoorraad is in het verleden te complex geacht. Een technische beperking kan een vorm van filtering of whitelisting zijn, maar ook beperking tot de personen woonachtig in een bepaald gebied.

[1] *Whitelisting is een beveiligingsmaatregel waarbij vooraf wordt vastgelegd van welke personen gegevens aan welke medewerker of directie verstrekt mogen worden. De gegevens van alle andere personen worden geblokkeerd of kunnen pas na verdere verificatie of toestemming worden verstrekt.*

1.2 Gegevenstoegang

Achtergrond

Met gegevenstoegang bedoelen we hier het verlenen van toegang tot een applicatie en daarin opgenomen gegevens. Dit wordt ook wel aangeduid als logisch toegangsbeheer of autorisatiebeheer. Voor de BRP betreft dit het verlenen van toegang tot het BRP-raadpleegscherm in Makelaarssuite en BenK-BRP met daarnaast het verlenen van toegang via de geautomatiseerde koppeling. Een geautomatiseerde koppeling met Makelaarssuite vergt toekenning van rechten in zowel de afnemende taakapplicatie als Makelaarssuite, de zogenaamde dubbele autorisatie. Bij gebruikmaking van BenK-BRP zal worden volstaan met toekenning van rechten in de taakapplicatie.

De toe te kennen autorisaties worden per directie afgesproken en vastgelegd in het transparantiedocument welke een bijlage bij het afnemersconvenant vormt. Autorisaties worden verleend op gegevensvelden.

Bevinding 3: Stedelijke processen logische toegangsbeheer niet nageleefd

In de gegevenstoegang tot de BRP worden verschillende onderdelen van het stedelijk proces logische toegangsbeheer niet nageleefd. De inrichting van de gegevenstoegang is door iedere directie vastgelegd in een actuele autorisatiematrix. In een autorisatiematrix wordt vastgelegd welke medewerkers toegang hebben tot welke applicaties en gegevens. Voor twee van de getoetste directies is vaststelling van de autorisatiematrix door de directie aantoonbaar. Bij de overige directies ontbreekt vaststelling van de autorisatiematrix.

In de autorisatiematrixen van alle directies is niet zichtbaar of de toegang tot deze gegevens is beperkt tot de organisatorische functies vermeld in het transparantiedocument.

Controles op toegekende rechten worden in overeenstemming met het stedelijk proces uitgevoerd. Er is echter niet vastgesteld dat constateringen van niet tijdig ingetrokken rechten hebben geleid tot een melding van een informatiebeveiligingsincident.

Functioneel Beheer verstrekt halfjaarlijks een rapportage van de resultaten van de uitgevoerde toegangscontroles voor het raadpleegscherm Makelaarssuite aan directie Data. Uit de rapportage over de toegangscontrole voor het eerste halfjaar van 2025 blijkt dat bij 37 van de 68 aansluitingen de rechten van medewerkers niet tijdig waren ingetrokken. De aantallen variëren van 1 medewerker tot 19 medewerkers per directie.

Bevinding 4: Beperkte aanvullende maatregelen voor toegang tot BRP-gegevens

In aanvulling op de stedelijke processen, kunnen directies aanvullende maatregelen treffen rond toegang tot BRP-gegevens. Dit vindt op dit moment beperkt plaats. Toegang tot de BRP-raadpleegschermen wordt door directie Data verleend na doorlopen van het stedelijk proces voor logisch toegangsbeheer waarbij de aanvraagbevoegde de aanvraag voor toekenning van rechten aangevuld met een door de gebruiker ondertekende akkoordverklaring BRP via de self servicedesk indient. Dit staat ook wel bekend als een aanvullende geheimhoudingsverklaring. De gebruiker verklaart hiermee bekend te zijn met de regels voor het gebruik van BRP-gegevens.

Medewerkers doorlopen echter geen training in de voorwaarden en regels voor omgang met BRP-gegevens voordat zij toegang krijgen tot deze gegevens.

Er is geen proces of activiteit aangetroffen gericht op intrekken van de toegang tot BRP-gegevens in geval van langere afwezigheid zoals sabbaticals of langdurige ziekte.

Risico

Het verkrijgen van toegang tot BRP-gegevens zonder training in de voorwaarden en regels voor omgang met BRP-gegevens verhoogt de kans op onrechtmatig raadplegen wat kan leiden tot datalekken.

Mogelijkheid tot toegang tot BRP-gegevens tijdens een periode van langere afwezigheid verhoogt de kans op ongezien onrechtmatig raadplegen wat kan leiden tot datalekken.

Mogelijke oorzaken

Basistaken zoals het tijdig intrekken van rechten worden niet beschouwd als belangrijk genoeg om in overeenstemming met de daarvoor stedelijk ingerichte processen uit te voeren.

Omgang met BRP-gegevens wordt niet herkend als omgang met gevoelige waardevolle gegevens, maar behandeld als onderdeel van de reguliere taakuitvoering.

Onvoldoende aandacht voor de gevolgen van bijzondere situaties voor andere aspecten van de werkzaamheden dan opvangen van de werkzaamheden van een langer niet beschikbare medewerker.

Best Practice - Gemeente Rotterdam

Rotterdam beperkt de toegang tot BRP-gegevens via twee kanalen: systematische toegang via taakapplicaties met strikt afgebakende datasets en handmatige toegang alleen wanneer dit functioneel noodzakelijk is. Gegevensvelden en datasets worden geclassificeerd op gevoeligheid en via een fijnmazige autorisatiestructuur toegewezen. Daarnaast werkt Rotterdam aan centrale logging en risicoprofielen voor proactieve monitoring, zoals het signaleren van ongebruikelijke of herhaalde bevragingen. Ook wordt transparantie versterkt door steekproeven vooraf aan te kondigen, casuïstiek bespreekbaar te maken en de zichtbaarheid van vertrouwenspersonen en integriteitscoördinatoren te vergroten.

1.3 Gebruik

Achtergrond

Nadat de gegevensverstrekking aan de directie is geregeld en medewerkers toegangsrechten hebben verkregen, kunnen medewerkers BRP-gegevens raadplegen. Deels kan dit in de taakapplicatie en deels moet dit in het BRP-raadpleegscherm.

Bevinding 5: Geen technische beperking zoekmogelijkheden tot toegewezen werk

Er ontbreekt een technische beperking van zoekmogelijkheden binnen de systemen. Dit betekent dat, zodra een medewerker geautoriseerd is, het technisch mogelijk is om persoonsgegevens van iedere persoon in de BRP te raadplegen, zonder dat een directe relatie met een toegewezen werkvoorraad aanwezig is, zoals een toegewezen dossier. Een dossier kan hier betekenen: een aanvraag voor een uitkering, een bezwaar tegen gemeentelijke heffingen, een verzoek om een betalingsregeling etc. Deze situatie betreft zowel de oude applicatie Makelaarssuite als de nieuwe applicatie BenK-BRP.

Bij alle directies zijn organisatorische afspraken aangetroffen over raadplegingen in het kader van de afhandeling van een (aanvraag)dossier of zaak. Bij een deel van de directies zijn ook afspraken aangetroffen over de registratie van de reden van bevraging. Voorbeelden van organisatorische afspraken zijn: alleen raadplegen voor toegewezen werk, niet jezelf raadplegen, niet een collega raadplegen, geen bekenden van jezelf of uit de media raadplegen.

In het BRP-raadpleegscherm wordt alleen een algemene reden voor de raadpleging vastgelegd, namelijk een taakaanduiding. Deze taakaanduiding is gekoppeld aan de naam van de medewerker die de gegevens opvraagt en geeft aan bij welk proces de raadpleging hoort. Medewerkers die toegang hebben tot meerdere processen, kunnen in ene menu een taakaanduiding kiezen. Het is echter niet mogelijk om in het scherm een koppeling te maken met een specifiek dossiercode of een verwijzing naar het toegewezen werk vast te leggen.

Risico

Door het ontbreken van technische beperkingen in mogelijkheden tot zoekmogelijkheden in de BRP-gegevens wordt de naleving van gegevensbescherming en privacyregels sterk afhankelijk van het gedrag en de integriteit van de medewerkers. Dit kan leiden tot een verhoogd risico op misbruik en maakt controle en toezicht moeilijker.

Het ontbreken van vermelding van bijvoorbeeld een dossiercode of een verwijzing naar toegewezen werk waarmee de raadpleging aan het toegewezen deel van de werkvoorraad kan worden gekoppeld, bemoeilijkt het houden van toezicht op de rechtmatigheid van raadplegingen. Dit kan ook leiden tot schending van de voorschriften uit de AVG en de BIO.

Ook bestaat het risico dat een medewerker in korte tijd grote hoeveelheden gegevens opvraagt om die op een later moment voor andere doeleinden te gebruiken.

Mogelijke oorzaken

- Organisatiekeuzes: in een deel van de stedelijke processen zijn medewerkers werkzaam voor de hele stad. Dit betreffen bijvoorbeeld medewerkers bij Dienstverlening (stadsloketten, CCA) en THOR (handhaving, toezicht). Echter, dit komt ook in voor andere processen waarbij een medewerker zelf een dossier ‘kiest’ (bijv. eerstvolgende nog niet behandelde dossier) uit een lijst van af te handelen dossiers.
- Technisch: er is geen koppeling van beschikbare dataset aan toegewezen werkpakket.

1.4 Toezicht

Achtergrond

Het sluitstuk van een goede beheersing van het rechtmatig raadplegen van persoonsgegevens wordt gevormd door toezicht, bijvoorbeeld door periodieke en proactieve monitoring en loganalyses op raadplegingen. Voor het kunnen uitoefenen van toezicht zijn een aantal randvoorwaarden noodzakelijk, zoals beschikbaarheid van relevante informatie en de volledigheid van loggegevens.

Bevinding 6: Actieve monitoring ontbreekt

Actieve monitoring door analyse van logbestanden wordt niet uitgevoerd. Logbestanden van raadplegingen in BRP-applicaties zijn aanwezig. Logbestanden van raadplegingen van BRP-gegevens in of via taakapplicaties zijn deels aanwezig. De logbestanden van de BRP-applicaties bevatten vermeldingen van gebruiker, moment van raadpleging (timestamp) en aanduiding taak. Zoals bij bevinding 1.3.1 vermeldt, wordt bij de raadpleging geen dossiercode vermeld.

Door het combineren van logbestanden uit de raadpleegapplicaties en de taakapplicaties is het mogelijk om een relatie te leggen tussen bevragingen van BRP-gegevens en redenen voor bevraging waar ook gebruik van wordt gemaakt voor onderzoek bij incidenten. Wel is hier sprake van een indirecte relatie tussen bestanden op basis van een combinatie gebruiker en tijdstip, omdat een aanduiding van dossiercode bij een bevraging ontbreekt.

In het onderzoek is geconstateerd dat actieve monitoring op raadplegingen van BRP-gegevens bij alle directies ontbreekt:

- Gestructureerde analyses van logbestanden vanuit de raadpleegmodule, eventueel gecombineerd met analyse van logbestanden uit taakapplicaties, vinden niet plaats.
- Er zijn ook geen overzichten of rapportages aangetroffen die laten zien dat er actief toezicht wordt gehouden of alertering worden gegeven op basis van IT-registraties voor het raadplegen van BRP-gegevens.

Leidinggevenden beschikken daardoor niet over objectieve gegevens waarmee ze kunnen nagaan of raadplegingen beperkt blijven tot legitieme bevragingen gerelateerd aan toegewezen taken.

Wel is geconstateerd dat directie Data is gestart met versterken van het toezicht op gebruik van persoonsgegevens. Dit naar aanleiding van aanbevelingen volgend uit het Beleidsonderzoek Gemeentelijk Corruptiebeleid van april 2024. De versterkingen bestaan uit een conceptprotocol voor periodieke toetsing van de naleving van de afspraken opgenomen in het leveringsconvenant. Deze periodieke toetsing heeft de vorm van een self-assessment. Eén van de toetsvragen betreft het uitvoeren van een periodieke toetsing naar de rechtmatigheid van de bevragingen. Directie Data is inmiddels ook gestart met het inrichten van een pilot met één van de afnemende directies (i.c. Wonen/vierde huis) voor het uitvoeren van een steekproef ter toetsing van de rechtmatigheid van de bevragingen.

Logs worden wel geanalyseerd naar aanleiding van een melding of incident (reactieve monitoring).

Risico

Als gevolg van het ontbreken van adequaat toezicht bestaat het risico dat medewerkers onopgemerkt en mogelijk langdurig BRP-gegevens raadplegen voor andere doeleinden dan de afhandeling van een toegewezen werktaak, bijvoorbeeld uit onwetendheid, nieuwsgierigheid of kwaadwillendheid.

Mogelijke oorzaken

- *Niet verzamelen en verwerken van de benodigde loggegevens. Benodigd zijn loggegevens uit meerdere applicaties, wat analyse van deze loggegevens compliceert.*
- *Ontbreken van gestructureerde analyse van raadplegingen en loggegevens in relatie tot reden van raadpleging op dossierniveau.*
- *Het ontbreken van een gegevensveld voor vastlegging van dossiercodering bij raadplegingen waardoor het leggen van een directe relatie met een toegewezen taak wordt bemoeilijkt*.

Best Practice - Politie

De politie monitort wekelijks het gebruik van persoonsgegevens door ruim 65.000 medewerkers te controleren via algoritmische analyses van logbestanden. Alle relevante raadplegingen worden uit meerdere systemen gecombineerd en beoordeeld met detectieregels die zijn gebaseerd op eerder misbruik. Voor iedere detectieregel wordt een score berekend die resulteert in een risicoscore per medewerker. Voorbeelden van gescoorde onderwerpen zijn bevragingen buiten werktijd of in het eigen woongebied. Een onafhankelijke toetsingscommissie, inclusief een OR-lid, beoordeelt de regels periodiek. Door een strikte scheiding tussen monitoring en onderzoek wordt de privacy van medewerkers beschermd.

Best Practice - AIB

De directies Werk & Participatie en Inkomen gebruiken Suwinet met een whitelist-systeem: medewerkers kunnen alleen gegevens raadplegen van personen met een lopende uitkeringsaanvraag. Raadplegingen buiten de whitelist vereisen een expliciete bevestiging. AIB voert maandelijks steekproeven uit op het gebruik, wat zowel controlerend werkt als bewustwording en bespreekbaarheid binnen teams vergroot. Onderzoek bestaat uit zoeken van verklaring in bestanden en navraag doen bij medewerkers voor verkrijgen van nadere verklaring van raadplegingen. Niet-verklaarbare raadplegingen worden als mogelijke integriteitsschending behandeld. Toegang is daarnaast gekoppeld aan strikte autorisatieprocedures en verplichte trainingen.

2. Soft controls

In deze audit worden beheersmaatregelen op het gebied van gedrag en cultuur aangeduid als soft controls. Er is onderzoek gedaan naar preventieve controls (helderheid, voorbeeldgedrag, betrokkenheid, uitvoerbaarheid), detectieve controls (transparantie, bespreekbaarheid) en responsieve controls (aanspreekbaarheid en bekrachtiging).

2.1. Preventieve soft controls

Achtergrond

Preventieve soft controls hebben als doel om onjuist gebruik van BRP-gegevens te voorkomen. Waar hard controls dit (systeemtechnisch) kunnen afdwingen, werken soft controls indirect via de normen, waarden en overtuigingen van medewerkers. In een ideale situatie is er een interactie tussen hard en soft controls waardoor deze elkaar versterken. In het geval van de preventieve soft controls is er raakvlak met de hard control thema's gegevensverstrekking, gegevenstoegang en gegevensgebruik. Voor deze thema's is vastgesteld dat medewerkers toegang kunnen krijgen tot de persoonsgegevens van alle inwoners van Amsterdam en zelfs van heel Nederland. Daarnaast zijn de mogelijkheden tot raadplegen niet beperkt met andere middelen dan de autorisatie. Dit betekent dat het technisch mogelijk is om onnodige raadplegingen te maken uit onwetendheid, nieuwsgierigheid en kwaadwillendheid. Preventieve soft controls kunnen medewerkers stimuleren om het gewenste gedrag te vertonen en daarmee het onjuist gebruik van BRP-gegevens voorkomen. De preventieve soft controls betreffen:

- **Helderheid** voor medewerkers die gebruikmaken van BRP-gegevens over wat gewenst en ongewenst gedrag is. Hoe helderder de verwachtingen, hoe beter zij begrijpen wat ze moeten doen, en hoe groter de kans dat ze dat ook écht doen.
- **Voorbeeldgedrag** van medewerkers en leidinggevenden die zelf zorgvuldig omgaan met BRP-gegevens. Hoe beter het voorbeeld dat in de gemeente wordt gegeven, hoe beter de werknemers zich gedragen.
- **Betrokkenheid** bij de organisatie en de afdeling, maar ook betrokkenheid tot de afgesproken omgang met BRP-gegevens. Hoe meer medewerkers zich onderdeel voelen van de organisatie en de afdeling en hoe meer zij zich kunnen vinden in de richtlijnen, hoe groter de kans dat zij zich volgens de richtlijnen gedragen.
- **Uitvoerbaarheid** van doelen, verantwoordelijkheden en taken. Hoe meer medewerkers beschikken over de juiste kennis en kunde over het gebruiken van de BRP-gegevens, hoe beter ze kunnen doen wat van hen wordt verwacht.

Tijdens de Quickscan (fase 1 van deze audit) hebben wij vastgesteld dat medewerkers de preventieve soft controls significant hoger scoorden dan de responsieve soft controls. Hieruit hebben wij geconcludeerd dat beïnvloedende maatregelen die gericht zijn op preventie van risico's in grotere mate aanwezig zijn dan gedrag beïnvloedende maatregelen gericht op respons. De groepsgesprekken die wij voor dit deel van het onderzoek hebben uitgevoerd laten deels een ander beeld zien. Het management geeft weliswaar aan dat er voldoende aandacht wordt besteed aan de preventieve maatregelen. In eerste instantie lijken de preventieve maatregelen in de ogen van de medewerkers ook aanwezig. Maar bij nadere doorvraag blijkt dit slechts in beperkte mate het geval te zijn. De kennis die er is lijkt veelal oppervlakkig. Dit resulteert in bevindingen voor elke preventieve soft control.

2.1.1. Helderheid

Bevinding 1: Niet iedere medewerker heeft bij aanvang van werkzaamheden de e-learning over de gedragscode gedaan.

Medewerkers die in dienst treden bij de gemeente Amsterdam zijn verplicht een aantal e-learnings te voltooien, waaronder de e-learning: Gedragscode Gemeente Amsterdam. In deze e-learning worden onder andere de gedragsregels rondom het omgaan met informatie behandeld. Echter, in meerdere directies wordt veel gewerkt met uitzendkrachten die vaak pas na één of twee jaar in dienst komen bij de gemeente. Deze uitzendkrachten krijgen de e-learning pas na verkrijgen van de vaste arbeidsovereenkomst met de gemeente, waardoor zij gedurende een langere periode zonder deze training in de systemen hebben gewerkt en mogelijk niet volledig op de hoogte zijn van de gedragsregels.

Bevinding 2: Onduidelijkheid over delen van BRP-gegevens tussen collega's.

Zowel leidinggevenden als medewerkers geven aan dat het duidelijk is wat de regels en richtlijnen zijn met betrekking tot het raadplegen en gebruiken van BRP-gegevens. Leidinggevenden geven ook aan dat deze duidelijk en periodiek gecommuniceerd Echter, wanneer bij medewerkers wordt doorgevraagd blijken er veel grijze gebieden te zijn. Een voorbeeld is het delen van informatie met collega's. Hierin lopen de werkwijzen dan ook uiteen tussen directies en afdelingen, maar ook blijkt binnen directies en afdelingen niet altijd duidelijk wat de werkwijze is. Voorbeelden van werkwijzen zijn: bij vragen van collega's verzoeken om de vraag te mailen zodat de reden van zoek achteraf aantoonbaar is, weigeren want collega heeft zelf toegang en anders geen recht op de informatie of parallel aan de collega zelf in het systeem gaan zoeken en op deze wijze 'meekijken'.

Risico

Als gevolg van het ontbreken van duidelijke richtlijnen en communicatie over gewenst en ongewenst gedrag bij het gebruik van BRP-gegevens, bestaat de kans dat medewerkers (onbewust) regels overtreden, waardoor de bescherming van gegevens en de naleving van wet- en regelgeving in gevaar komt.

Mogelijke oorzaken

- *In de procedure voor het aannemen van uitzendkrachten is niet opgenomen dat zij de e-learning volgen.*
- *De aanwezige richtlijnen over de omgang met BRP-gegevens staan niet op papier en worden niet structureel en periodiek gecommuniceerd*.

2.1.2. ***Voorbeeldgedrag***

Bevinding 3: Voorbeeld vanuit leidinggevenden wordt niet als zodanig herkend.

Medewerkers ervaren beperkt voorbeeldgedrag van hun hiërarchisch leidinggevenden wat betreft omgang met gegevens uit de BRP. Er is een discrepantie tussen het (voorbeeld)gedrag dat leidinggevenden zeggen te vertonen en hoe dat door medewerkers wordt ervaren. De goede gedragingen die de leidinggevenden laten zien, worden niet gekoppeld aan de omgang met de BRP. Medewerkers geven aan dat dit niet zichtbaar is als gevolg van de afstand tussen medewerkers en de leidinggevenden en omdat het goede voorbeeld niet specifiek genoeg is, het heeft niet direct raakvlak met de omgang met BRP-gegevens.

Risico

Als gevolg van het niet ervaren van het goede voorbeeld van leidinggevenden door medewerkers, bestaat de kans dat medewerkers minder het belang inzien van een goede omgang met de BRP-gegevens, waardoor regels minder goed worden nageleefd en het risico op ongewenst gedrag toeneemt.

Mogelijke oorzaken

- *Leidinggevenden zijn in de meeste gevallen zelf niet inhoudelijk bekend met de daadwerkelijke uitvoering van de werkzaamheden waarvoor BRP-gegevens worden geraadpleegd. Daarnaast opereren zij in de ogen van de medewerkers op grote afstand van de medewerker. Hierdoor wordt het goede voorbeeld niet gezien, of is het niet specifiek genoeg waardoor medewerkers geen vertaalslag maken naar hun eigen werk.*
- *De manier van aandacht besteden aan omgang met BRP-gegevens wordt door medewerkers niet als zodanig ervaren. Leidinggevenden geven in de gesprekken aan dat zij op verschillende manieren aandacht besteden aan de manier waarop met de vertrouwelijke gegevens wordt omgegaan. Medewerkers geven echter aan dat er geen aandacht wordt besteed.*

2.1.3 Betrokkenheid

Bevinding 4: Ondanks dat men achter de richtlijnen staat, worden raadplegingen gedaan om andere redenen dan uitvoering van toegewezen taken.

Medewerkers geven aan zich betrokken te voelen bij het goed en vertrouwelijk omgaan met BRP-gegevens. Desondanks wordt door sommige medewerkers ook aangegeven dat zij vanuit nieuwsgierigheid of voor privégebruik soms een bepaalde raadpleging doen. Het bewustzijn van het belang van een goede omgang met BRP-gegevens is niet altijd in toereikende mate aanwezig en medewerkers voelen niet altijd genoeg erkenning voor hun rol. Daardoor is een raadpleging uit nieuwsgierigheid of een privéraadpleging in de ogen van sommige medewerkers te rechtvaardigen.

Risico

Als medewerkers zich onvoldoende betrokken voelen bij hun werk of het belang van een goede omgang met BRP-gegevens, bestaat de kans dat zij ook minder belang hechten aan de voorgeschreven werkwijze, waardoor hun motivatie en bereidheid om zorgvuldig om te gaan met BRP-gegevens afneemt of zelfs ontaardt in misbruik en/of oneigenlijk gebruik van persoonsgegevens.

Mogelijke oorzaken

Medewerkers geven aan dat het niet altijd duidelijk is wat de gevolgen zijn van slechte hygiëne met betrekking tot BRP-gegevens. Daarnaast wordt soms aangegeven dat een hoge werkdruk in combinatie met een gebrek aan erkenning leidt tot een lagere betrokkenheid tot het werk in het algemeen.

2.1.4 Uitvoerbaarheid

Bevinding 5: Training bij aanvang is vooral gericht op inhoud en minder op omgang met BRP-gegevens.

Uit de gesprekken blijkt dat medewerkers bij de start van hun functie wel worden getraind voor vakinhoudelijke taken, maar dat omgang met BRP-gegevens hierin nauwelijks aandacht krijgt. Enkel via de e-learning over de gedragscode worden zij op de hoogte gebracht van gewenst gedrag in omgang met gevoelige gegevens.

Ook worden medewerkers ingewerkt door ervaren collega's, maar zonder gebruik van een uniform inwerkprogramma, een simulatieomgeving en dummygegevens

Bevinding 6: Systeemproblemen, systeembeperkingen en werkdruk leiden tot onzorgvuldigheid.

Medewerkers geven aan dat als gevolg van problemen met IT-systemen, gebreken in de systeeminrichting en werkdruk soms keuzes worden gemaakt die strijdig zijn met de gemeentelijke richtlijnen voor informatiebeveiliging, privacybescherming en daarmee ook strijdig met de regels voor het gebruik van BRP-gegevens. Een voorbeeld hiervan is het met elkaar delen van wachtwoorden om efficiënter te kunnen werken.

Risico

Als gevolg van het ontbreken van voldoende kennis, middelen of ondersteuning bij medewerkers, bestaat de kans dat medewerkers niet in staat zijn om hun taken met betrekking tot BRP-gegevens correct uit te voeren, wat kan resulteren in fouten of misbruik.

Mogelijke oorzaken

- *Omgang met BRP-gegevens wordt niet herkend als omgang met gevoelige waardevolle gegevens, maar behandeld als onderdeel van de reguliere taakuitvoering.*
- *Trainingsmateriaal is ontoereikend*
- *Ontbreken van een Dummy, waardoor medewerkers de eigen registratie raadplegen om iets uit te kunnen leggen.*
- *Werking van het systeem is niet helder. Om vast te stellen of er een storing is, wordt snel de eigen registratie geraadpleegd.*
- *Keuze van de medewerkers en de organisatie om bij inlogproblemen te kiezen voor een alternatieve, pragmatische, oplossing zoals delen van wachtwoorden om de omvang van de werkvoorraden beheersbaar te houden, ook al gaat dit ten koste van naleving van wet- en regelgeving op gebied van privacybescherming en informatiebeveiliging.*

2.2 Detectieve soft controls

Achtergrond

De hard controls rondom BRP-gegevens zijn binnen de gemeente ingericht om het rechtmatig gebruik van deze BRP-gegevens te borgen, onder andere via autorisaties en periodieke controles. Uit de bevindingen blijkt echter dat deze maatregelen in de praktijk vooral reactief functioneren: leidinggevenden hebben geen direct zicht op het raadpleeggedrag van medewerkers, logging wordt niet structureel benut voor toezicht en structurele proactieve monitoring ontbreekt. Hierdoor ontstaat er beperkt zicht op wat medewerkers daadwerkelijk doen in de systemen. Om dit gebrek aan zicht enigszins te dempen, zijn de detectieve soft controls van groot belang. De detectieve soft controls betreffen

- **Transparantie** van gedrag. Hoe beter zichtbaar is wat medewerkers doen, hoe meer ze geneigd zijn zich te houden aan de afgesproken werkwijze omtrent het gebruik van BRP-gegevens.
- **Bespreekbaarheid** van standpunten, emoties, dilemma's en overtredingen omtrent het gebruiken van de BRP-gegevens. Hoe meer ruimte medewerkers hebben om te praten over morele kwesties, hoe meer zij dit ook daadwerkelijk doen en hoe meer ze hierbij leren van anderen. Daarbij biedt dit leidinggevenden inzicht in wat er speelt op de werkvloer.

2.2.1. Transparantie

Bevinding 7: Beperkt zicht op raadpleeggedrag van medewerkers

Uit de interviews blijkt dat het zicht van zowel leidinggevenden als collega's op het raadplegen en gebruiken van BRP- gegevens door medewerkers beperkt is. Beiden geven aan dat ze niet kunnen zien welke bevragingen collega's uitvoeren of met welke persoonsgegevens zij werken. Het daadwerkelijke gebruik van systemen is alleen zichtbaar wanneer iemand fysiek meekijkt, wat in de praktijk nauwelijks voorkomt. Deze bevinding sluit aan bij de uitkomsten van de QuickScan. Zowel in de QuickScan als in dit verdiepende onderzoek is vastgesteld dat er nauwelijks inzicht is in het feitelijke raadpleeggedrag van medewerkers. Hierdoor worden afwijkingen niet preventief gesignaleerd, maar pas zichtbaar wanneer zich een incident voordoet.

Risico

Als gevolg van het beperkte zicht op het raadpleeggedrag van medewerkers bestaat het risico dat onrechtmatige of oneigenlijke raadplegingen van BRP-gegevens niet tijdig worden gesignaleerd. Afwijkend gedrag kan hierdoor langere tijd onopgemerkt blijven. Dit vergroot de kans op misbruik van persoonsgegevens en schending van privacy van burgers. Daarnaast belemmert het ontbreken van transparantie leidinggevenden in hun rol om effectief toezicht te houden en tijdig bij te sturen.

Mogelijke oorzaken

Beperkt zicht op de raadplegingen door medewerkers en collega's is deels inherent aan het zelfstandig werken aan een werkvoorraad, maar wordt deels ook veroorzaakt door het ontbreken van objectieve informatie over BRP-raadplegingen zoals moment van raadplegen, reden van raadplegen en hoeveelheid raadplegingen.

2.2.2 Bespreekbaarheid

Bevinding 8: Wisselende bespreekbaarheid van knelpunten en gedrag in teamverband

Uit de interviews blijkt dat zowel door de medewerker als de leidinggevende de bespreekbaarheid rondom het gebruik van BRP-gegevens wisselend wordt ervaren. Medewerkers geven aan dat zij bij knelpunten, twijfels of grijze gebieden in de uitvoering vaak eerst een (meer ervaren) collega of senior benaderen om te overleggen. Deze gesprekken blijven echter meestal informeel en individueel, waardoor situaties niet structureel worden teruggekoppeld of benut als leermoment voor het team als geheel.

Leidinggevenden geven in de interviews aan dat bespreekbaarheid binnen hun teams aanwezig is en dat medewerkers met vragen, twijfels en dilemma's bij hen terecht kunnen. Sommige leidinggevenden benoemen dat casuïstiek anoniem wordt besproken. Tegelijkertijd blijkt uit de g

Best Practice - Rijksrecherche

Transparantie - Herhaalde of ongebruikelijke raadplegingen, zoals het opzoeken van dezelfde persoon, familieclusters of personen buiten de gemeente, kunnen belangrijke signalen zijn van misbruik.

onderwerp BRP-gebruik niet overal een vast onderdeel is in de overleggen. Hierdoor ontstaat een verschil tussen de ervaren openheid vanuit de leidinggevenden en de beleving van medewerkers.

Deze bevinding sluit aan bij de uitkomsten van de QuickScan. Hieruit bleek dat medewerkers over het algemeen voldoende ruimte ervaren om dilemma's en gevoelige onderwerpen te bespreken, maar dat leidinggevenden kwesties rondom de verwerking van BRP-gegevens niet altijd actief en zichtbaar bespreekbaar maken in teamverband. Zowel de QuickScan als dit verdiepende onderzoek laten zien dat bespreekbaarheid wel aanwezig is, maar niet structureel, niet specifiek gericht op de verwerking van BRP-gegevens, niet eenduidig en sterk afhankelijk van de persoon.

Risico

Twijfels, grijze gebieden en mogelijk ongewenste gedrag rondom het gebruik van BRP-gegevens wordt niet in breed verband besproken, waardoor het leereffect voor het team uitblijft, onjuiste werkwijzen kunnen blijven bestaan en de kans wordt vergroot dat medewerkers onbedoeld regels overtreden. Ook bestaat de kans dat signalen over kwetsbare situaties van medewerkers (zoals mogelijke schulden of problemen in hun privé) te laat of helemaal niet bij de hiërarchische leidinggevenden terechtkomen met als gevolg een toename in het risico op afgedwongen onrechtmatige raadpleging van BRP-gegevens.

Mogelijke oorzaken

- *Het ontbreken van vaste, structurele momenten voor bespreking van dilemma's, knelpunten en incidenten rondom het gebruik van BRP-gegevens zoals in werkoverleggen en bila's.*
- *Door de afstand tussen leidinggevenden en de dagelijkse uitvoering hebben leidinggevenden beperkt zicht op het feitelijke gebruik van systemen en weinig concrete aanknopingspunten om het gesprek over BRP-gebruik gericht te voeren.*
- *Het ontbreken van structurele en objectieve informatie over de omgang met BRP-gegevens.*
- *Wederzijds ongemak over het bespreken van privéomstandigheden van medewerkers. Deels voortkomend uit behoefte aan privacy en het respecteren van iemands behoefte aan privacy. Deels ook voortkomend uit andere factoren zoals schaamte en niet weten hoe risicovolle omstandigheden en mogelijke gevolgen van levensgebeurtenissen aan de orde te stellen.*

2.3 Responsieve soft controls

Uit de hard control bevindingen blijkt dat actieve monitoring ontbreekt, loggegevens vooral worden geanalyseerd naar aanleiding van incidenten, en leidinggevenden geen direct zicht hebben op het raadpleeggedrag van medewerkers. Hierdoor worden mogelijke overtredingen of ongewenste gedrag vaak pas zichtbaar nadat een incident heeft plaatsgevonden.

Responsieve soft controls zijn nauw verbonden met deze hard controls. Wanneer de hard controls niet op niveau zijn, heeft dit een negatieve invloed op de werking van soft controls. Tegelijkertijd zijn goede responsieve soft controls randvoorwaardelijk voor een effectieve werking van de hard controls. De responsieve soft controls betreffen:

Aanspreekbaarheid op fouten, incidenten en calamiteiten omtrent het gebruiken van de BRP-gegevens. Hoe veiliger medewerkers zich voelen met dingen melden, of met het direct aanspreken van anderen in de gemeente, hoe meer zij dit ook daadwerkelijk zullen doen en hoe meer ze van deze situaties leren.

Bekrachtiging door middel van het waarderen - of zelfs belonen - van gewenst gedrag en het bestraffen van ongewenst gedrag omtrent het gebruikmaken van de BRP-gegevens. Hoe beter de handhaving, hoe meer medewerkers zullen neigen naar wat wordt beloond en vermijden wat wordt bestraft.

2.3.1 Aanspreekbaarheid

Bevinding 9: Beperkt en niet structureel aanspreken op gedrag in omgang met BRP-gegevens

Uit de interviews met zowel medewerkers als leidinggevenden blijkt dat aanspreekbaarheid rondom het gebruik van BRP-gegevens wisselend wordt ingevuld. Medewerkers spreken elkaar vooral aan op zichtbaar gedrag, zoals het niet vergrendelen van een laptop, omgang met dienstmiddelen of wat iemand op de werkplek laat liggen. Aanspreken op het feitelijke raadpleeggedrag in systemen vindt nauwelijks plaats, omdat dit voor collega's en leidinggevenden niet zichtbaar is.

Leidinggevenden geven aan dat zij medewerkers aanspreken wanneer er signalen, meldingen of incidenten zijn met betrekking tot onnodige raadplegingen. In de dagelijkse praktijk is aanspreken echter niet overal een vast onderdeel van de aansturing. In sommige teams gebeurt dit tijdens bila's of naar aanleiding van concrete voorvallen, terwijl het bij andere teams nauwelijks aan bod komt. Medewerkers geven bijvoorbeeld aan dat identiteitsbewijzen niet direct worden vernietigd na inname (conform richtlijnen) en dat hier niets over wordt gezegd. Het beeld is daarmee sterk afdelings- en persoonsafhankelijk.

Deze bevinding sluit aan bij de resultaten van de QuickScan. Daaruit kwam naar voren dat medewerkers het melden van afwijkingen als serieus ervaren, maar minder positief zijn over de waardering voor het elkaar corrigeren op gedrag. Dit bevestigt het beeld dat aanspreken wel gebeurt, maar niet structureel wordt gestimuleerd of genormaliseerd binnen teams.

Risico

Door het ontbreken van structurele aanspreekbaarheid bestaat het risico dat onjuist of oneigenlijk gebruik van BRP-gegevens niet tijdig wordt gecorrigeerd. Wanneer aanspreken zich vooral beperkt tot zichtbare gedragingen en niet tot het daadwerkelijke systeemgebruik, kunnen overtredingen langere tijd ongecorrigeerd blijven. Dit vergroot de kans op versterking van ongewenst gedrag en maakt dat normen over zorgvuldig omgaan met persoonsgegevens worden verzwakt binnen teams.

Mogelijke oorzaken

- *Het gebrek aan inzicht in het daadwerkelijke raadpleeggedrag van medewerkers. Doordat leidinggevenden en collega's geen inzicht hebben in welke bevragingen worden gedaan, ontbreekt het belangrijkste triggersignaal om elkaar hierop aan te spreken. Aanspreken blijft daardoor beperkt tot gedragingen die fysiek zichtbaar zijn of naar aanleiding van een incident.*
- *Het ontbreken van het bespreken van de omgang met BRP-gegevens als vast agendapunt (zie bespreekbaarheid) bemoeilijkt ook de uitvoerbaarheid van het op een als veilig ervaren wijze van aanspreken van medewerkers bij het waarnemen van afwijkingen, dilemma's of twijfelgevallen*
- *Twijfel bij de medewerker over de juistheid van de eigen interpretatie van regels. Hier zien we dat gebreken in preventieve soft controls de uitvoerbaarheid van responsieve soft controls bemoeilijken.*
- *Terughoudendheid bij medewerkers om collega's aan te spreken door onvoldoende informatie van daadwerkelijke gedragingen.*

2.3.2 Bekrachtiging

Bevinding 10: Bekrachtiging vindt plaats bij ernstige gevallen

Uit de interviews met leidinggevenden blijkt dat handhaving plaatsvindt wanneer zich concrete overtredingen of incidenten voordoen. Leidinggevenden geven aan dat medewerkers worden aangesproken bij geconstateerd niet-integer of niet-functioneel gedrag en dat in ernstige gevallen maatregelen worden genomen. Medewerkers weten ook dat zware overtredingen consequenties kunnen hebben, zoals ontslag.

Tegelijkertijd blijkt uit zowel de interviews met leidinggevenden als de QuickScan dat handhaving en bekrachtiging in de praktijk vooral naar aanleiding van incidenten plaatsvinden. Veelal gaat dit om ernstige gevallen die niet aan het licht komen door onderzoek vanuit de leidinggevenden, maar door meldingen of onderzoek van het openbaar ministerie. Ook geven medewerkers aan dat zowel grenzen als consequenties niet duidelijk gecommuniceerd worden. Hierdoor verliest de handhaving de afschrikkende werking.

Daarnaast komt uit de gesprekken naar voren dat positieve bekrachtiging van zorgvuldig omgaan met persoonsgegevens beperkt en niet structureel plaatsvindt. Complimenten worden vooral gegeven op algemeen functioneren, omgangsvormen en werkinhoud, en nauwelijks op zorgvuldig gebruik van persoonsgegevens. De QuickScan bevestigt dit beeld. Hierdoor ontstaat het beeld dat bekrachtiging wel bestaat, maar niet structureel en niet zichtbaar betrekking heeft op het dagelijks gedrag rondom BRP-gebruik.

Risico

Doordat bekrachtiging vooral plaatsvindt naar aanleiding van grote incidenten zijn de consequenties niet goed zichtbaar, bestaat het risico dat ongewenst gedrag onvoldoende wordt gecorrigeerd en gewenst gedrag onvoldoende wordt gestimuleerd. Medewerkers kunnen hierdoor het gevoel krijgen dat afwijkend gedrag wordt gedoogd. Dit vergroot de kans dat regels rondom het gebruik van BRP-gegevens niet consequent worden nageleefd.

Daarnaast verzwakt het ontbreken van zichtbare en consequente handhaving de integriteitscultuur. Als grenzen niet duidelijk worden gecommuniceerd en zorgvuldig handelen niet actief wordt gewaardeerd of beloond, vermindert de normerende werking op het gedrag van medewerkers. Dit vergroot het risico dat overtredingen blijven plaatsvinden.

Mogelijke oorzaken

- *Informatie voor het uitoefenen van structureel en proactief toezicht op het gebruik van BRP-gegeven ontbreekt.*
- *Het is voor medewerkers en leidinggevenden niet altijd duidelijk welke consequenties verbonden zijn aan welke soorten overtredingen (zoals zware overtredingen of twijfelgevallen). Protocollen hiervoor ontbreken, waardoor het per team en per leidinggevende verschilt hoe bekrachtiging wordt ingevuld.*
- *Waardering en beloning van zorgvuldig gedrag zijn geen expliciet onderdeel van de aansturing. Complimenten worden af en toe gegeven (dit verschilt ook per leidinggevende), maar vooral op algemeen werkgedrag en niet specifiek op zorgvuldige omgang met BRP-gegevens. Hierdoor wordt gewenst gedrag onvoldoende zichtbaar versterkt.*

Best Practice - Openbare Orde en Veiligheid

De Basistraining Ondermijning verhoogt het bewustzijn van medewerkers over mogelijke signalen van ondermijning, zoals corruptie en situaties waarin ambtenaren in contact kunnen komen met potentiële criminelen. Het bewustzijn en alertheid op mogelijke veiligheidsrisico's binnen het werk verschilt per afdeling door variatie in aandacht voor integriteit, inwerkprogramma's en specifieke diploma's. Tijdens de training wordt door deelnemers aangegeven dat het dagelijks gebruik van belangrijke systemen en omgaan met gevoelige informatie soms kan leiden tot een afname van alertheid. Ook kan een te groot vertrouwen op organisatorische maatregelen, zoals controles en het vier-ogenprincipe, een gevoel van schijnveiligheid creëren als deze maatregelen niet consistent worden toegepast. In de training komen regelmatig aandachtspunten naar voren die betrekking hebben op de weerbaarheid van medewerkers, zoals het gebruik van initialen en achternamen van medewerkers in externe communicatie, het ontbreken van communicatie over logging als preventieve werking en de vindbaarheid en benaderbaarheid van individuele medewerkers op social media.

3. Best Practices

In het onderzoek zijn gesprekken gevoerd met zowel interne als externe professionals die te maken hebben met BRP-gegevens. In dit hoofdstuk beschrijven we de best practices die we binnen en buiten de gemeente hebben verzameld en geven we aan welke lessen kunnen worden getrokken om de beheersing van het gebruik van BRP-gegevens verder te verbeteren op de aspecten: hard controls en soft controls.

3.2. Advisering Interne Beheersing - Suwinet

De directie Werk en Participatie en de directie Inkomen maken voor hun werkzaamheden gebruik van Suwinet. In Suwinet zijn persoonsgegevens uit de BRP verrijkt met bezitsgegevens uit RDW, de Rijksbelastingdienst en het Kadaster. De applicatie wordt gebruikt voor toetsing van aanvragen voor uitkeringen op juistheid van opgegeven inkomen en vermogen. De medewerkers zijn daarom bevoegd tot raadplegen van gegevens van personen waarvoor een aanvraag voor een uitkering is geregistreerd. Deze personen zijn in de applicatie opgenomen in een whitelist. Wanneer een medewerker persoonsgegevens wil raadplegen van iemand die niet op de whitelist staat, wordt expliciet gevraagd of de raadpleging gewenst is.

Daarnaast voert AIB maandelijks steekproeven uit naar het legitieme gebruik van Suwinet. De afwijkingen van deze steekproef spreekt de leidinggevende met de betrokken medewerker om uit te zoeken of er een verklaring voor de raadpleging kan worden gevonden.

De maandelijkse steekproeven hebben niet alleen een controlerende functie, maar zorgen er ook voor dat het onderwerp binnen teams bespreekbaar wordt. Dit draagt bij aan een cultuur van bewust en zorgvuldig omgaan met Suwinet. Wanneer een raadpleging niet kan worden verklaard, wordt de casus verder behandeld als een mogelijke integriteitsschending en wordt het daarvoor bestaande proces gestart.

Om medewerkers te ondersteunen, is er uitgebreide informatie beschikbaar via een intranetpagina, inclusief werkinstructies voor leidinggevenden. Het is gebleken dat goed getrainde leidinggevenden een belangrijke rol spelen in het voorkomen van onrechtmatige raadplegingen. Toegang tot Suwinet is daarnaast gekoppeld aan strikte autorisatieprocedures, waarbij medewerkers een e-learning moeten volgen en een examen moeten afleggen.

3.3. Politie – Protective Monitoring

De politie controleert structureel de rechtmatigheid van de geraadpleegde persoonsgegevens van alle 65.000 politieambtenaren. Dit gebeurt via een algoritmische analyse, ook wel Protective Monitoring genoemd, waarbij logs uit meerdere relevante systemen worden geanalyseerd. Deze monitoring geldt voor alle politieambtenaren, ongeacht rang, functie of interne of externe positie.

De detectie vindt wekelijks plaats en omvat een analyse van de afgelopen drie maanden voor alle applicaties die onder monitoring vallen. De resultaten van deze analyse worden omgezet in een objectieve score, gebaseerd op variabelen zoals bevragingen buiten werktijden of in het eigen woongebied. De detectieregels zijn gebaseerd op eerdere gevallen van misbruik en worden continu geëvalueerd en aangepast. Elke detectieregel bevat een weegfactor die aangeeft hoe ernstig een overtreding wordt beoordeeld.

Om toezicht te houden op de detectieregels is een toetsingscommissie ingesteld, waarin ook een OR-lid zitting heeft om het perspectief van de medewerker te waarborgen.

De privacy van medewerkers wordt beschermd door een strikte scheiding tussen de monitoring en het daaropvolgende onderzoek en verdere afhandeling.

3.4. Gemeente Rotterdam

De gemeente Rotterdam heeft de toegang tot BRP-gegevens beperkt tot twee distributiekanalen: systematische toegang via taakapplicaties en handmatige toegang, vergelijkbaar met het Amsterdamse Raadpleegscherm. Bij systematische toegang zijn de gegevenssets en -velden strikt beperkt tot wat noodzakelijk is voor de uitvoering van specifieke taken, gebaseerd op een autorisatiesystematiek met meerdere gradaties en classificatie van persoonsgegevens op gevoeligheid. Handmatige toegang tot alle BRP-gegevens wordt alleen verleend wanneer dit essentieel is voor de functie.

Daarnaast werkt gemeente Rotterdam aan een nieuwe koppeling tussen taaksystemen en applicaties van andere gemeentelijke afnemers, waarbij gebruik wordt gemaakt van API's vanuit BRP-V, om gegevensuitwisseling efficiënter te maken.

Verder is een project gestart om logging centraal te organiseren en risicoprofielen te ontwikkelen voor proactieve monitoring, zoals het signaleren van meerdere bevragingen op één BSN of raadplegingen op ongebruikelijke tijdstippen.

Tot slot benadrukt de gemeente Rotterdam het belang van het vooraf aankondigen van steekproeven om transparantie te vergroten, het bespreken van casuïstiek uit de media om bewustwording te stimuleren, en het verbeteren van de zichtbaarheid en communicatie rondom de beschikbaarheid van vertrouwenspersonen en integriteitscoördinatoren.

3.5. Openbare Orde en Veiligheid - Ondermijningstraining

De afdeling Amsterdamse aanpak ondermijning biedt de Basistraining Ondermijning aan voor alle medewerkers van de organisatie. De training heeft als doel medewerkers bewust te maken van mogelijke signalen van ondermijning, onder meer door praktijkvoorbeelden te geven van corruptie en situaties waarin ambtenaren in contact kunnen komen met potentiële criminelen. Uit eigen waarneming door de trainers blijkt dat de training bijdraagt aan een groter bewustzijn

van ondermijning en corruptierisico's, hoewel dit bewustzijn per afdeling kan verschillen. Sommige afdelingen besteden meer aandacht aan onderwerpen zoals integriteit en training dan andere. Daarnaast spelen factoren zoals de inhoud van het inwerkprogramma en het hebben van specifieke diploma's een rol in de alertheid op mogelijke veiligheidsrisico's binnen het werk. Tijdens de training wordt door deelnemers aangegeven dat het dagelijks gebruik van belangrijke systemen en omgaan met gevoelige informatie soms kan leiden tot een afname van alertheid. Ook kan een te groot vertrouwen op organisatorische maatregelen, zoals controles en het vier-ogenprincipe, een gevoel van schijnveiligheid creëren als deze maatregelen niet consistent worden toegepast. In de training komen regelmatig aandachtspunten naar voren die betrekking hebben op de weerbaarheid van medewerkers, zoals het gebruik van initialen en achternamen van medewerkers in externe communicatie, het ontbreken van communicatie over logging als preventieve werking en de vindbaarheid en benaderbaarheid van individuele medewerkers op social media.

3.6. Rijksrecherche

De Rijksrecherche signaleert verschillende knelpunten in de huidige inrichting van de systemen van de gemeente Amsterdam en benadrukt de volgende punten voor verbetering:

- Logging toont momenteel alleen wie gegevens heeft geraadpleegd, maar niet waarom of welke specifieke gegevens zijn bekeken.
- Lokale raadpleging van BRP-gegevens wordt lokaal gelogd, terwijl directe raadpleging in de BRP-V zorgt voor centrale logging bij de Rijksdienst voor Identiteitsgegevens (RvIG). Centrale logging bij de RvIG is essentieel voor de Rijksrecherche om analyses uit te voeren na incidenten.
- Er is vaak geen volledig overzicht van alle applicaties waarin raadplegingen plaatsvinden, waardoor niet alle logging kan worden geanalyseerd. Het ontbreken van een volledig overzicht beperkt de mogelijkheden om misbruik effectief te signaleren.

Daarnaast benadrukt de Rijksrecherche het belang van een goede relatie tussen leidinggevenden en medewerkers. Dit contact speelt een cruciale rol in de afweging of de medewerker een benadering door het criminele circuit meldt.

Naarmate overtredingen voortduren, wordt de kans kleiner dat een medewerker naar de politie stapt. Daarom is het belangrijk om aan de voorkant te waarborgen dat elke benadering, hoe pril of voorzichtig ook, wordt gedeeld.

Ook wordt opgemerkt dat de incidenten vaker gelinkt kunnen worden aan ambtenaren die langer in dienst zijn, maar door persoonlijke omstandigheden vatbaarder kunnen worden voor criminele beïnvloeding.

De Rijksrecherche heeft daarnaast enkele patronen geïdentificeerd die kunnen wijzen op misbruik van BRP-gegevens. Voorbeelden hiervan zijn:

- Het periodiek opzoeken van dezelfde persoon (raadpleegtreintjes);
- Het 'googlen' in de BRP, bijvoorbeeld door dezelfde naam te raadplegen met steeds een ander geboortejaar;
- Het frequent raadplegen van personen buiten de gemeente Amsterdam;
- Het opzoeken van meerdere familieleden binnen dezelfde familie.

Bijlage 1: Hard en soft controls

Hard controls

Hard controls zijn formele, tastbare maatregelen die zijn ontworpen om de verstrekking, toegang, het gebruik en het toezicht op BRP-gegevens te waarborgen. Hard controls vormen de basis voor het waarborgen van een rechtmatige omgang met BRP-gegevens.

Voorbeelden van hard controls zijn:

- **Beleid en procedures**: Het opstellen van duidelijke richtlijnen en protocollen voor de verstrekking van gegevens;
- **Technische beperkingen**: Het toepassen van bijvoorbeeld filters of whitelisting om toegang tot gegevens te beperken tot wat strikt noodzakelijk is voor de uitvoering van specifieke taken;
- **Logisch toegangsbeheer**: geformaliseerd proces voor het toekennen, wijzigen of intrekken van rechten op toegang tot informatie en informatiesystemen;
- **Autorisatiematrix**: Een overzichtelijk schema, vastgesteld door de proceseigenaar, dat vastlegt welke gebruiks(groepen) toegang hebben tot functies, gegevens of systemen, eventueel gegroepeerd in rollen of profielen. Het overzicht toont gebruikersrechten en toegestane acties zoals lezen, schrijven, bewerken en verwijderen;
- **Toegangscontrole**: Het regelmatig controleren van toegangsrechten op toekenning van de juiste rechten aan de juiste personen. Bij afwijkingen volgt melding als informatiebeveiligingsincident en correctie van de rechten;
- **Beperkingen op zoekmogelijkheden**: Het technisch beperken van zoekopdrachten tot alleen de gegevens die nodig zijn voor toegewezen taken;
- **Registratie van gebruik**: Het vastleggen van de reden voor gegevensraadpleging, bijvoorbeeld door het koppelen van een dossiercode aan elke raadpleging;
- **Logging**: Het bijhouden van logbestanden waarin wordt vastgelegd wie, wanneer en waarom gegevens heeft geraadpleegd;
- **Monitoring en rapportage**: Het analyseren van logbestanden en het opstellen van rapportages om afwijkingen of misbruik te signaleren.

Soft controls

Soft controls spelen een essentiële rol in het gedrag en de houding van medewerkers en leidinggevenden. Soft controls zijn informele, niet-tastbare factoren binnen een organisatie die het gedrag van medewerkers beïnvloeden en bijdragen aan het behalen van organisatiedoelen. Ze richten zich op de cultuur, normen, waarden, en de intrinsieke motivatie van medewerkers.

De acht gehanteerde soft controls zijn:

- **Helderheid** voor medewerkers die gebruikmaken van BRP-gegevens over wat gewenst en ongewenst gedrag is.
- **Voorbeeldgedrag** van medewerkers en leidinggevenden die zelf zorgvuldig omgaan met BRP-gegevens.
- **Betrokkenheid** bij de organisatie en de afdeling, maar ook betrokkenheid tot de afgesproken omgang met BRP-gegevens.
- **Uitvoerbaarheid** van doelen, verantwoordelijkheden en taken.
- **Transparantie** van gedrag.
- **Bespreekbaarheid** van standpunten, emoties, dilemma's en overtredingen omtrent het gebruiken van de BRP-gegevens.
- **Aanspreekbaarheid** op fouten, incidenten en calamiteiten omtrent het gebruiken van de BRP-gegevens.
- **Bekrachtiging** door middel van het waarderen - of zelfs belonen - van gewenst gedrag en het bestraffen van ongewenst gedrag omtrent het gebruikmaken van de BRP-gegevens.

De wisselwerking tussen hard en soft controls

De relatie tussen hard controls en soft controls is essentieel voor de effectieve beheersing van omgang met persoonsgegevens. Soft controls kunnen namelijk de werking van hard controls versterken door gewenst gedrag te stimuleren, ongewenst gedrag tegen te gaan en een bijdrage leveren in het tijdig signaleren van risico's. Wanneer er sterke hard controls aanwezig zijn, maar de soft controls ontbreken, kan dit leiden tot schijnveiligheid. Medewerkers begrijpen bijvoorbeeld niet waarom bepaalde regels bestaan of voelen zich niet betrokken, waardoor de naleving van de regels in gevaar komt. Aan de andere kant, als er sterke soft controls zijn maar de hard controls ontbreken, kan een cultuur van bewustzijn en verantwoordelijkheid weliswaar risico's verminderen, maar blijft de organisatie kwetsbaar door het ontbreken van structurele waarborging van rechtmatige omgang met BRP-gegevens. Een goede balans tussen hard en soft controls is daarom essentieel om zowel technische als gedragsmatige risico's effectief te beheersen.

Bijlage 2: Scope en verantwoording werkzaamheden

Scope

De audit richt zich op bevoegden met toegangsrechten tot de BRP binnen de gemeente Amsterdam. Voor de tweede fase van het onderzoek zijn de volgende directies geselecteerd op basis van het aantal medewerkers dat persoonsgegevens kan raadplegen: Belastingen,

Dienstverlening, Werk en Participatie, Inkomen en Toezicht Handhaving Openbare Ruimte (THOR).

In deze audit onderzoeken we expliciet de beheersmaatregelen ter borging van bevoegd en uitsluitend voor uitvoering van gemeentelijke processen raadplegen van persoonsgegevens rechtstreeks in iBurgerzaken of door ter beschikking stelling in Makelaarssuite.

Niet in scope

- Raadpleging van BRP-gegevens door onbevoegden anders dan via functionaliteit van gebruikte gemeentelijke applicaties (bijv. hacking e.d.);
- Overheidsinstanties buiten de gemeente Amsterdam;
- Overige basisregistraties zoals BAG en BRV;
- Directies binnen de gemeente Amsterdam met een laag aantal bevoegden met raadpleegfuncties op de BRP zoals: de Stadsdelen, Juridisch Bureau, Grond en Ontwikkeling en de GGD;
- Processen voor onderhouden van (authentieke) persoonsgegevens in de BRP;
- Het raadplegen van persoonsgegevens via het distributiekanaal: het verstrekken van bestanden.
- Onderzoek naar mogelijke onrechtmatige raadpleging van BRP-gegevens.

Verantwoording werkzaamheden

Deze audit is uitgevoerd in overeenstemming met het Audit Charter 2024, welke is ondertekend door de Gemeentesecretaris. Hierin staat de reikwijdte van onze werkzaamheden en bevoegdheden beschreven en deze is te vinden op de intranetpagina van IA&BO. Onze werkzaamheden worden uitgevoerd in overeenstemming met de normen van de beroepsgroep voor interne auditors. Dit is het Instituut voor Interne Auditors (IIA). Sinds september 2022 is IA&BO gecertificeerd.